UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of

A BLACK SAMSUNG CELL PHONE ASSIGNED IMEI # 355796460738812

Case No. 2:24-sw-0571 CKD

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

SEE ATTACHMENT A-3, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed *(identify the*

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251	Production of Child Pornography
18 U.S.C. § 2252(a)(2)	Receipt of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography
18 U.S.C. § 1470	Transfer of Obscene Material to Minors
18 U.S.C. § 2422(b)	Coercion or Enticement of a Minor

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☑ Continued on the attached sheet.

/s/
Applicant's signature

Loretta M. Bush, Special Agent - FBI
Printed name and title

Sworn to me and signed telephonically.

Date: June 3, 2024 at 8:30 am

Carolyn K. Delaney
Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, Chief U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Loretta M. Bush, being sworn to tell the truth, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since May 2016. I am presently assigned to the Tampa Division's Sarasota Resident Agency's Child Exploitation and Human Trafficking Task Force. In this capacity, I am responsible for conducting criminal investigations of statutes contained in Title 18 of the United States Code, including crimes related to child sex trafficking, child pornography and the sexual exploitation of children, among other violations of federal law.

2. From March 2021 to the present, I have worked crimes against children violations in the Tampa Division. I have participated in investigations of persons suspected of violating federal child pornography and child sex trafficking laws, including 18 U.S.C. §§ 2251, 2252, 2422, and 1591. These investigations have included the use of surveillance techniques, the interviewing of subjects and witnesses, and the planning and execution of arrest, search, and seizure warrants. In the course of these investigations, I have reviewed images and videos containing child pornography and images depicting minor children engaged in sexually explicit conduct on various forms of electronic media including computers, digital cameras, and wireless telephones, and have discussed and reviewed these materials with other law enforcement officers. I have also received multiple trainings on crimes against children matters.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of the **TARGET DEVICE**, which was located in Buddy Allen TRAVIS' ("**TRAVIS**") possession and was seized pursuant to a federal arrest warrant.

4. The **TARGET DEVICE** is a black Samsung cell phone assigned IMEI # 355796460738812. The **TARGET DEVICE** is currently located at the Federal Bureau of Investigation, Sacramento FBI office, 2001 Freedom Way, Roseville, California 95678, and are more particularly described in **Attachment A**. **Attachment A** is incorporated by reference.

5. The applied-for search warrant would authorize the forensic examination of the **TARGET DEVICE** for the purpose of identifying electronically stored data particularly described in **Attachment B**. **Attachment B** is incorporated by reference. As set forth in more detail below, there is probable cause to believe that **TRAVIS** has violated 18 U.S.C §§ 2251 (production of child pornography), 2252(a)(2) (receipt of child pornography), 2252(a)(4)(B) (possession of child pornography), 1470 (transfer of obscene material to minors), and 2422(b) (coercion or enticement of a minor), and evidence of the offenses will be found on the **TARGET DEVICE**.

6. The facts contained in this affidavit are drawn from personal knowledge based on my participation in this investigation, information from other criminal

investigators, information from law-enforcement officers, information from agency reports, and the review of documents provided to me by witnesses and by law enforcement officers. Because this affidavit is being submitted for the limited purpose of seeking authorization to search the **TARGET DEVICE**, I have not set forth each and every fact learned during the course of this investigation.

DEFINITIONS

7. The following definitions apply to this Affidavit and **Attachment B**:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of 18.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short to enable other participants to respond quickly in a format that resembles an oral conversation. This feature distinguishes "chatting" from other text-based online communications, such as, internet forums and email.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) to include any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a

minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct.

e. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means that are capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

f. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

g. "Computer passwords and data security devices," as used herein, consists of information or items designed to restrict access to or to hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (*i.e.*, a string of alphanumeric and/or other characters) usually operates a sort of digital key to "unlock" particular data security devices. Data

security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

h. "Fingerprint sensor-enabled device" refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and to verify their identity.

i. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, electronic mail ("email"), remote storage, and co-location of computers and other communications equipment.

j. "Mobile applications," as used herein, are specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including, such as, engaging in online chat, reading a book, or playing a game.

k. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

TECHNICAL TERMS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Secure Digital ("SD") – A SD card is commonly used as the digital memory storage device/computer disk within certain electronic devices, such as cellular telephones. In addition to cellular telephones being able to make telephone calls and send text messages, many modern cellular telephone (also known as Smartphones) have the ability to browse the internet, download and store images and videos, and take photographs and videos with built in digital cameras. SD cards can store images, videos, and various other digital media and files. SD cards can be easily removed from one compatible electronic device and used in another and in computers. Individuals can use portable, wireless tablets (for example, an Apple iPad, a Samsung Galaxy, and even certain models of iPods) to take pictures, record videos, and send that media over email, text messages, or even a messaging service; all of which can then be synchronized to a computer.

c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

9. Based on my training, experience, and research, I know that the **TARGET DEVICE** has capabilities that allows it to serve as a wireless telephone, digital camera, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

PROBABLE CAUSE

10. On July 19, 2023, the FBI received information that **TRAVIS**, an adult male residing in Vacaville, California, requested sexually explicit images and videos from a minor female victim, ("VICTIM"), who currently resides in Bradenton, Florida. VICTIM is currently fifteen years' old.

11. On or about June 12, 2023, VICTIM's father reported to the Bradenton Police Department (BPD) that he and his wife searched VICTIM's cell phone and located images of an erect male penis contained within the photo gallery section. Additionally, VICTIM's mother located a Facebook Messenger chat between VICTIM and **TRAVIS**, an individual known to the parents.

12. BPD reviewed VICTIM's cell phone with her parent's consent. During

the review, BPD located a chat thread between VICTIM's Facebook account and **TRAVIS'** Facebook account which contained multiple images of VICTIM, both clothed and unclothed, exposing her breasts and vagina. BPD also located videos of VICTIM masturbating and images of an erect penis and an adult male, identified as **TRAVIS**.

13. BPD also observed multiple instances of audio and video calls between VICTIM's Facebook account and **TRAVIS'** Facebook account and conversations discussing the VICTIM traveling to California to visit **TRAVIS**.

14. BPD screen-recorded the chat to preserve the conversation. The chat began in April 2023.

15. On or about June 30, 2023, with the consent of VICTIM's parents, BPD conducted a complete digital extraction of VICTIM's cell phone.

16. On or about August 7, 2023, I took custody of the VICTIM's cell phone and entered it into evidence at the FBI. I also obtained a copy of the digital extraction, and the screen recording of the Facebook Messenger chats between VICTIM's Facebook account and **TRAVIS'** Facebook account.

17. During the review of the screen recorded Facebook Messenger chat, I observed child sexual abuse material (CSAM). Furthermore, I observed that the Facebook Messenger chats between VICTIM's account and **TRAVIS'** Facebook account occurred between approximately April 2023 and June 2023.

///

FACEBOOK MESSENGER CHATS

18. I located the following excerpt from May 15, 2023:

TRAVIS: **Okay. Send me all you naughty pics**

VICTIM: actually?

TRAVIS: Sure

VICTIM: lmao ok (VICTIM sends 4 images depicting the victim in a bra, exposing her stomach, bent over sticking her buttock out)

VICTIM: i have more i deleted the actual decent ones i had bc my friend was going through my camera roll

TRAVIS: Ahhh

VICTIM: (Victim sends 3 images of her clothed, stomach is exposed)

TRAVIS: Should turn the flash off

VICTIM: [laughing/tears emoji]

VICTIM: next time i will

TRAVIS: **What your breast look like**

TRAVIS: I've seen alot bit not yours lol

VICTIM: lmao hold on let me look through my camera roll

19. On or about May 22, 2023, **TRAVIS'** Facebook account sent an image of an adult male, wearing glasses, a backwards ballcap, and a yellow t-shirt with his chest and stomach exposed. The adult male is using one of his hands to lift his shirt up to expose his stomach and chest. (The VICTIM's parents identified the individual

in the image as **TRAVIS**.) The VICTIM responded by sending an image of her exposed breasts. **TRAVIS'** Facebook account responded by sending an image depicting an erect adult penis.

20. I located the following excerpt from May 22, 2023, following a 13-minute video chat (for which no content was retained):

TRAVIS: Ya. I hit off on your boons

TRAVIS: Got^

TRAVIS: Noobs^

VICTIM: lmaoo

TRAVIS: Boobs

TRAVIS: Ya.... ya

TRAVIS: I was trying to involve you but social media.is.more important

VICTIM: one of the next couple times it will be in person.

VICTIM: i didn't know that you should of said that

TRAVIS: Promise

VICTIM: yes [praying hands emoji]

TRAVIS: Shouldn't should not have said things went out the window a week ago

VICTIM: whatt

VICTIM: ok now i see why you get confused when i message you when i'm drunk lol

TRAVIS: Ya cause you just said...i didn't know that you should of said that

VICTIM: ohhh

VICTIM: see i'm not all the way in my head right now it wasn't processing

TRAVIS: Your not doing anything you haven't wanted to

VICTIM: i know

TRAVIS: You also gotnto see something that you have wanted too

TRAVIS: I know. He takes his own bows

TRAVIS: Thank you..thank you

VICTIM: mhm

TRAVIS: So we done and sleep time. Or you wanna go further

VICTIM: what do you mean

TRAVIS: **I wanna see all of you. You keep playing coy**

TRAVIS: Disregard that I'm drunk I apologize

21. I located the following excerpt from June 2, 2023:

TRAVIS: Are you still up?

VICTIM: Mhm

TRAVIS: **I listen to you getting off. But Wana see it**

TRAVIS: 1 sec.

TRAVIS: You there?

VICTIM: Ya. I don't show that thoughhh

VICTIM: Im bored.

TRAVIS: So show me

TRAVIS: **I'm hard and wanna**

TRAVIS: **I want to see your mouth around this**

TRAVIS: [**TRAVIS'** FACEBOOK ACCOUNT sends an image of an erect penis being held by the individual's hand.]

VICTIM: Mmmmmm

TRAVIS: [attempts an audio call]

VICTIM: Call me back in 5 mins

VICTIM: Actually like 2 mins

TRAVIS: Bet

TRAVIS: I'm calling

TRAVIS: [Missed audio call]

VICTIM: [There was a video chat for 4 minutes]

VICTIM: My phone is being weird.

VICTIM: Your audio keeps cutting out

VICTIM: I think its my airpods

VICTIM: [VICTIM sends an image of herself. The image depicts VICTIM from her neck down to her hips. She is wearing a black bra and black jeans.]

TRAVIS: Beautiful

TRAVIS: Show me were you want to put this

TRAVIS: [**TRAVIS'** Facebook account sends an image of an erect penis.]

VICTIM: Ok ok how about this i fr dont send pictures like that but i can send you smt similiar but it wont exactly be what you want

TRAVIS: Well.. let's see

VICTIM: [thumbs up emoji]

VICTIM: [VICTIM sends an image that depicts a nude female from the naval to the knees. The vagina is visible. The female is laying on her back on a bare mattress.]

TRAVIS: Mmmm

TRAVIS: [Missed audio call]

VICTIM: Ya

VICTIM: [VICTIM sends an image that depicts a nude female from above the naval to the knees. The vagina is visible. The female is laying on her back on a bare mattress.]

TRAVIS: [33-minute audio call]

VICTIM: Whats upp

TRAVIS: I was told I was being loud

VICTIM: By who

TRAVIS: My current roommate

VICTIM: [Laughing/crying emoji]

TRAVIS: What ever

VICTIM: Did he hear anything?

TRAVIS: Ni

VICTIM: Ok good

VICTIM: Fuck. This whole thing was so awesome

VICTIM: Im gonna go to sleep I'm so tired.

VICTIM: I love you

22. I located the following excerpt from June 12, 2023:

TRAVIS: Xvideo

VICTIM: [sends an image of a female laying on her back on a bare mattress. The female is nude from the navel down. The vagina is visible.]

VICTIM: [sends an image of a female laying on her back on a bare mattress. The female is nude from the navel down. The vagina is visible.]

VICTIM: [sends a 5 second video of a female laying on her back on a bare mattress. The female is nude from the navel down. The vagina is visible. The female uses her hand to masturbate.]

23. Based on the Facebook Messenger chats, law enforcement determined that the Facebook user ID for the Facebook account belongings to **TRAVIS**.

24. On or about December 6, 2023, the FBI conducted a forensic interview of VICTIM. A Child and Adolescent Forensic Interviewer ("CAFI") interviewed VICTIM and confirmed that VICTIM understood the difference between the truth and a lie.

25. VICTIM confirmed talking to **TRAVIS** through Facebook Messenger for approximately one year. VICTIM believed she was in a relationship with **TRAVIS**. VICTIM explained that the conversations began normally and turned sexual with **TRAVIS** asking her to send "nudes" of herself to **TRAVIS**. **TRAVIS**

told VICTIM that "it was in his nature" or that it was "because he was a man" that he was asking VICTIM for nude photographs. VICTIM described these statements as disturbing. VICTIM stated that **TRAVIS** asked for pictures of her "boobs" and "vagina" and for sexual videos of VICTIM. VICTIM admitted to sending **TRAVIS** sexual pictures and videos of herself through Facebook Messenger. VICTIM explained that she had never sent images or videos of her "bottom" half before sending them to **TRAVIS** and stated that she felt forced to send the material to **TRAVIS**. VICTIM also confirmed receiving sexual images and videos of **TRAVIS**. VICTIM stated that **TRAVIS** sent her pictures of his penis and videos of **TRAVIS** "jerking off", which VICTIM said meant that **TRAVIS** was masturbating.

26. On February 12, 2024, a federal search warrant was executed on **TRAVIS'** Facebook account. A review of the search warrant return revealed that **TRAVIS'** Facebook account contained a portion of the Facebook Messenger Chats that were previously located on the VICTIM's cell phone.

27. On April 2, 2024, a federal search warrant was executed on the VICTIM's Facebook account. A review of the search warrant return revealed that the VICTIM's Facebook account contained the full version of the Facebook Messenger Chats that were previously located on the VICTIM's cell phone.

28. On May 2, 2024, a federal grand jury in the Middle District of Florida, returned an indictment charging **TRAVIS** with coercion and enticement of a minor to engage in sexual activity, in violation of 18 U.S.C. § 2422(b), production of child

pornography, in violation of 18 U.S.C. § 2251(a), receipt of material involving the sexual exploitation of a minor, in violation of 18 U.S.C. § 2252(a)(2) and transfer of obscene material to a minor, in violation of 18 U.S.C. § 1470.

29. On May 14, 2024, pursuant to a federal arrest warrant out of the Middle District of Florida, **TRAVIS** was located and arrested at the Extended Stay, 799 Orange Dr. Vacaville, California. The **TARGET DEVICE** was in **TRAVIS'** possession.

30. After seizing the **TARGET DEVICE**, I observed an image of a digitally styled cartoon cat on the home screen that was similar in nature to the profile picture on **TRAVIS'** Facebook account. The **TARGET DEVICE** was entered into evidence at the FBI.

31. On May 14, 2024, during a post-Miranda interview with **TRAVIS'**, **TRAVIS** admitted to knowing the VICTIM and to using a Facebook account that was registered in his true name, "Buddy Travis", which is consistent with the Facebook Messenger Chats with the VICTIM.

32. Based on the foregoing information, there is probable cause to believe that the **TARGET DEVICE** may contain evidence, fruits, and/or are instrumentalities of the violations described above.

///

///

///

BACKGROUND ON COMPUTERS, DEVICES, AND CHILD SEX ABUSE MATERIAL

33. Based on my training and experience, I know that individuals who engage in sexual exploitation of minors often also collect and produce child sex abuse material.

34. Computer technology has revolutionized the way in which individuals interested in child sex abuse material interact with each other. Child sex abuse material was once produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and to reproduce the images. There were definable costs involved with the production of pornographic images. Consequently, distributing such media on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. Distribution, accordingly, was accomplished through a combination of personal contacts, mailings, and telephone calls. The development of computers has changed this. Now, computers serve multiple functions in connection with child pornography, including, principally: production, communication, distribution, and storage.

35. Child pornographers can now transfer photographs onto a computer-readable format with a scanner. With the advent of digital cameras, they can now also transfer such images directly onto a computer. A device known as a modem allows any computer to connect to another computer by telephone, cable, or wireless

connection. Such electronic contact can connect literally millions of computers around the world.

36. A computer and cellphone's ability to store images in digital form makes the computer, itself, an ideal repository for child pornography. Within the last decade, the size of the electronic storage media, commonly known as a hard drive, on home computers has grown tremendously. Consequently, cellphones and hard drives can now easily store thousands of images at very high resolution.

37. The Internet affords collectors of child sex abuse material several different venues to obtain, view, and/or trade child sex abuse material in a relatively secure and anonymous fashion.

38. Collectors and distributors of child sex abuse material also use online resources to retrieve and to store child sex abuse material, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Often, evidence of such online storage of child sex abuse material is also found on the user's computer. Even in cases where online storage is used, however, evidence of child sex abuse material can still be found on the user's computer in most cases.

39. Digital files, such as, movies and pictures, can also be easily transferred between computers, smart phones, and other devices, or stored simultaneously on

multiple devices. Collectors of child sex abuse material often keep their child pornography in multiple places, including on multiple devices.

40. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*e.g.*, by saving an e-mail as a file on the computer or by saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be unintentionally retained (*e.g.*, traces of a path of an electronic communication may be automatically stored in many places, such as, in temporary files or ISP client software). In addition to electronic communications, a computer user's activities on the Internet generally leave traces, "footprints," and/or history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

41. Cellular phones and cellular phone technology have further revolutionized the way in which individuals interested in child pornography interact with each other. Today's cellular phones, many of which are called "smart phones," are typically capable of storing a wide variety of data. Such data includes not only telephone numbers, contact lists, addresses, voicemails, and/or text messages, but also images, videos, documents, and programs (often referred to as "applications" or "apps") in much the same way a desktop or laptop computer does.

42. Data can also be stored on a cellular phone, particularly when it has a high-storage capacity, just like a computer. The storage capacity for a cellular phone includes both internal and removable digital memory. Today's cellular phones can offer up to 128 gigabytes of storage, or more. Removable memory storage can significantly increase, if not double, that storage capacity. As a result, cellular phones can store thousands of high-resolution images and videos. Further, the phones have the ability to be synced with, or connected to, a computer, which allows the user to transfer files between the devices.

43. Cellular phones are also typically able to access the Internet through either a wireless data plan and/or through a wireless (also known as "wi-fi") Internet connection. This allows cellular phone users to perform many Internet functions on their phones, such as, downloading and uploading data (*e.g.*, images, videos) from the Internet, sending and receiving emails, accessing web pages, browsing the Internet, using instant messaging services, and conducting live video chat. Consequently, cellular phones—given their ability to access the Internet and to download images and/or videos onto its internal and removable digital memory—are ideal repositories for child pornography, just like computers, and provide child pornographers with an additional method to share and to trade their child pornography collections.

44. Cellular phones can also take pictures or "images," which are stored as image files, such as, "JPEGs" or "TIFFs." Image files often contain Exchangeable Image File Format ("EXIF") data. EXIF data can include a variety of information

about the image, including, for example, the time and date that the image was taken, the place where an image was taken (also known as "geolocation data"), the settings that the device used to capture the image, the model of the camera phone that was used to take the image, the focal length of the lens, aperture settings, shutter speed, and ISO speed.

DEVICES AND COMPUTER DATA

45. As detailed above, there is probable cause to believe that **TRAVIS** used the **TARGET DEVICE** in furtherance of 18 U.S.C §§ 2251 (production of child pornography), 2252(a)(2) (receipt of child pornography), 2252(a)(4)(B) (possession of child pornography), 1470 (transfer of obscene material to minors), and 2422(b) (coercion or enticement of a minor), and those records and information will be stored on the **TARGET DEVICE**. Thus, the warrant applied for would authorize the seizure of the **TARGET DEVICE** under Federal Rule of Criminal Procedure 41(e)(2)(B).

46. In my training and experience, records might be found on a computer's hard drive or other storage media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

47. Based on my knowledge, training, and experience, and consultation with other law-enforcement agents, I know that computer files or remnants of such

files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten, also known as free space or slack space. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

48. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. It is technically possible, however, to delete this information.

49. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard-drive space devoted to these files,

and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

50. As further described in **Attachment B**, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

51. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as, word processor, picture, and movie files), computer storage media can contain other forms of electronic evidence, such as, the following:

a. Forensic evidence of how computers were used, the purpose of their use, who used them, and when they were used, as described further in **Attachment B**, called for by this warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the

computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs (and associated data) that are designed to eliminate data may be relevant to establishing the user's knowledge or intent.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

52. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

53. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to

draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

54. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

55. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

56. I know that when an individual uses an electronic device to entice a minor to engage in criminal sexual conduct and to request and/or receive visual depictions of a minor engaged in sexually explicit conduct, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic

device was used; data that was sent or received; and other records that indicate the nature of the offense.

57. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether either is evidence described by the warrant.

58. *Manner of execution.* Because this warrant seeks only permission to examine the device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. There is good cause to execute this search warrant at any time, day or night, because the TARGET DEVICE is in law enforcement possession and its forensic examination may occur at any time during the day or night.

///

///

///

///

CONCLUSION

59. Based on the above information, probable cause exists that the **TARGET DEVICE**, as fully described in **Attachment A**, contain evidence, fruits,

and/or instrumentalities of violations of 18 U.S.C §§ 2251 (production of child pornography), 2252(a)(2) (receipt of child pornography), 2252(a)(4)(B) (possession of child pornography), 1470 (transfer of obscene material to minors), and 2422(b) (coercion or enticement of a minor). Accordingly, I respectfully request a warrant to search the **TARGET DEVICE** and seize the items listed in **Attachment B**.

/s/
Loretta Bush, Special Agent
Federal Bureau of Investigation

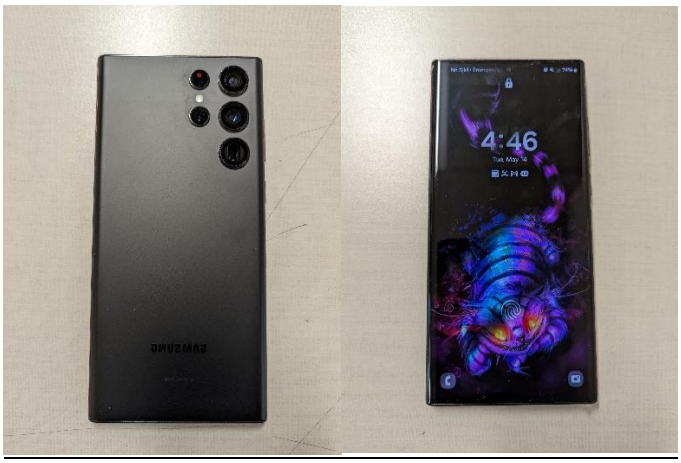
Affidavit submitted to me by reliable electronic means and attested to me as true and accurate by telephone or other reliable electronic means consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) before me this 3rd day of June 2024.

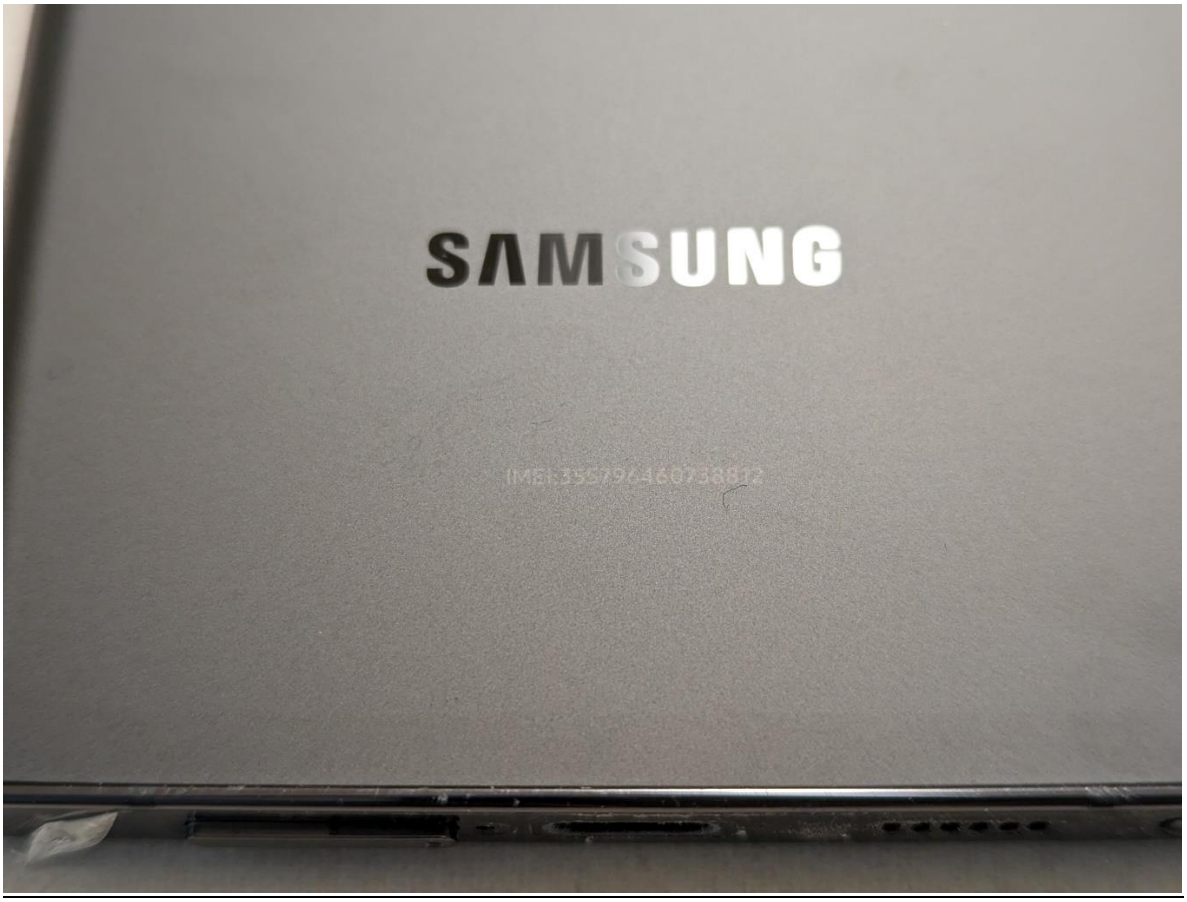
HONORABLE CAROLYN K. DELANEY
United States Magistrate Judge

/s/ Nicholas M. Fogg
Approved as to form by
AUSA NICHOLAS M. FOGG

ATTACHMENT A
Item to be Searched

A black Samsung cell phone assigned IMEI # 355796460738812, ("**TARGET DEVICE**"). The **TARGET DEVICE** is currently located at the Sacramento FBI office, 2001 Freedom Way, Roseville, California 95678. Pictures of the device are located on the next page.


4:46


SAMSUNG

ATTACHMENT B
List of Items to be Seized and Searched

A. Particular thing to be searched:

The property to be searched is the **TARGET DEVICE**, as described in **Attachment A**.

B. Information to be seized:

1. All records that relate to violations of 18 U.S.C. §§ 2251, 2252, 2422 and 1470 involving Buddy Allen TRAVIS, consisting of the following:

2. All visual depictions, including still images, videos, films, or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

3. Any and all documents, photographs, videos, records, emails, text communications, voicemail messages, location services (GPS data), contacts, logs, caches, and internet history pertaining to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, relating to an interest in child pornography, whether transmitted or received; pertaining to an interest in child exploitation, child erotica, pedophilia, or sexual abuse of children; relating to the persuading, inducing, enticing, or coercing of minors to engage in prostitution or any sexual activity; or pertaining to the transfer of obscene matter to minors.

4. Any and all passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

5. Any and all computer data that would reveal the presence of malware, viruses, or malicious codes located on the computer storage media.

6. Any and all records, documents, invoices, and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, and electronic messages, as well as other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

7. Any documents, records, programs, or applications relating to the existence of counter-forensic programs (and associated data) that are designed to eliminate data from cellular phones.

8. Evidence of user attribution showing who used or owned the **TARGET DEVICE** at the time the events described in this warrant occurred, such as logs, documents, internet searches, and browsing history.

9. Any records or information about Internet Protocol addresses accessed or used by the **TARGET DEVICE**.

10. Evidence the **TARGET DEVICE** was attached to any other storage devices or similar containers for electronic evidence, to include other devices that connected via Bluetooth, direct connection, Airdrop, or another Wi-Fi/ Bluetooth enabled sharing app or capability between devices.

11. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage such as on a SIM card, SD card, and any photographic form.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of A BLACK SAMSUNG CELL PHONE ASSIGNED IMEI # 355796460738812	)	Case No. 2:24-sw-0571 CKD

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of California *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before June 17, 2024 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: June 3, 2024 at 8:30 am

Carolyn K. Delaney

Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, Chief U.S. Magistrate Judge

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

_____

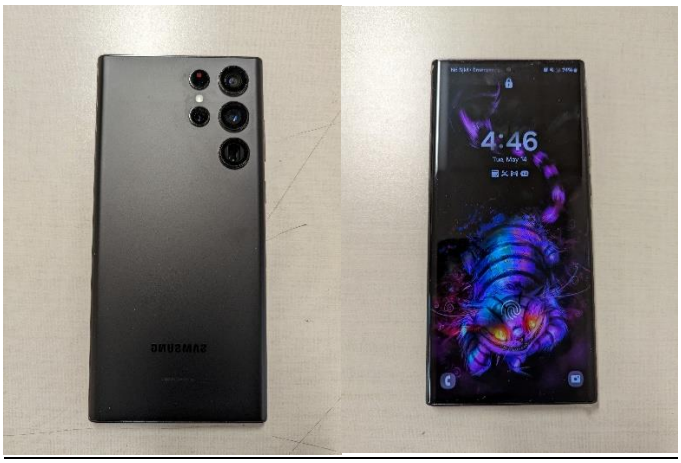
Subscribed, sworn to, and returned before me this date.

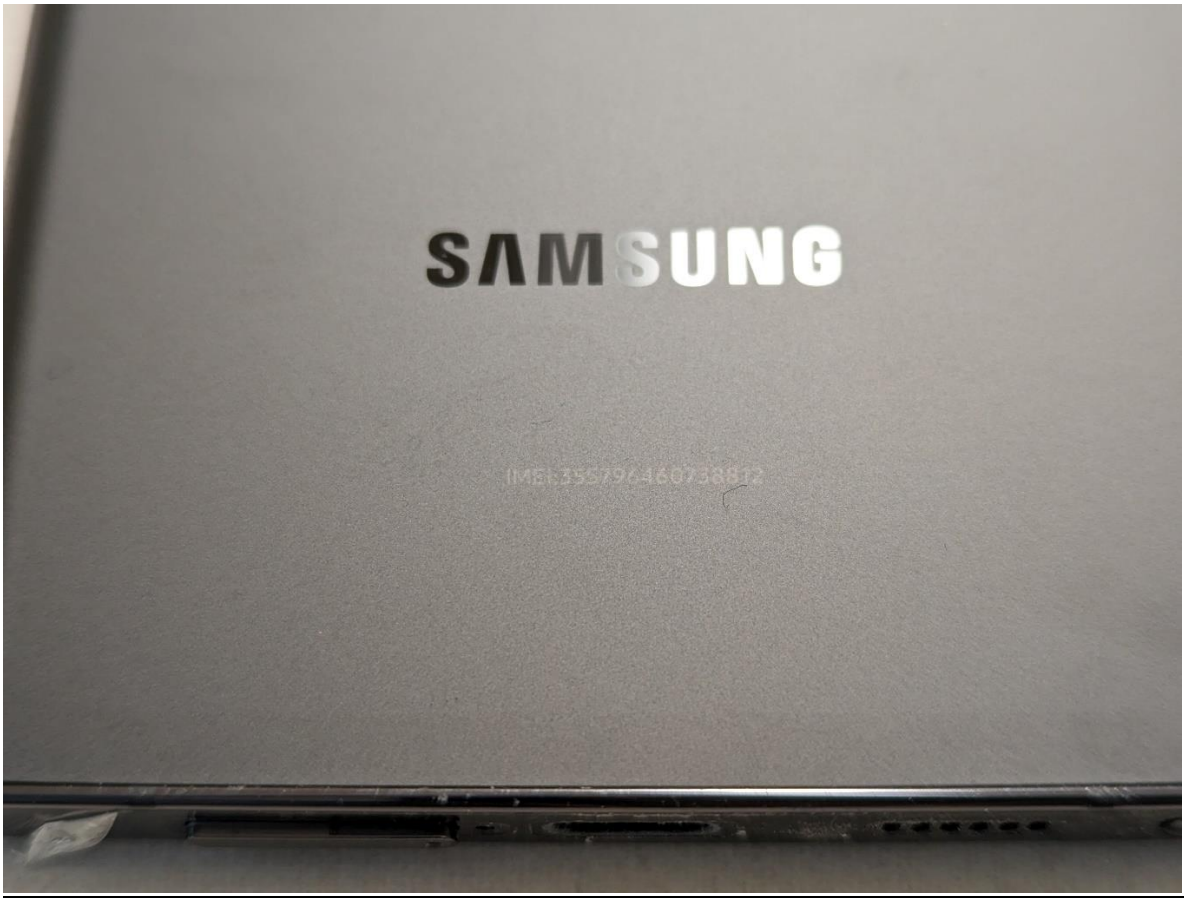
_____ _____

Signature of Judge Date

ATTACHMENT A
Item to be Searched

A black Samsung cell phone assigned IMEI # 355796460738812, ("**TARGET DEVICE**"). The **TARGET DEVICE** is currently located at the Sacramento FBI office, 2001 Freedom Way, Roseville, California 95678. Pictures of the device are located on the next page.


4:46


SAMSUNG

ATTACHMENT B
List of Items to be Seized and Searched

A. Particular thing to be searched:

The property to be searched is the **TARGET DEVICE**, as described in **Attachment A**.

B. Information to be seized:

1. All records that relate to violations of 18 U.S.C. §§ 2251, 2252, 2422 and 1470 involving Buddy Allen TRAVIS, consisting of the following:

2. All visual depictions, including still images, videos, films, or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

3. Any and all documents, photographs, videos, records, emails, text communications, voicemail messages, location services (GPS data), contacts, logs, caches, and internet history pertaining to the production, possession, receipt, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, relating to an interest in child pornography, whether transmitted or received; pertaining to an interest in child exploitation, child erotica, pedophilia, or sexual abuse of children; relating to the persuading, inducing, enticing, or coercing of minors to engage in prostitution or any sexual activity; or pertaining to the transfer of obscene matter to minors.

4. Any and all passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

5. Any and all computer data that would reveal the presence of malware, viruses, or malicious codes located on the computer storage media.

6. Any and all records, documents, invoices, and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, and electronic messages, as well as other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

7. Any documents, records, programs, or applications relating to the existence of counter-forensic programs (and associated data) that are designed to eliminate data from cellular phones.

8. Evidence of user attribution showing who used or owned the **TARGET DEVICE** at the time the events described in this warrant occurred, such as logs, documents, internet searches, and browsing history.

9. Any records or information about Internet Protocol addresses accessed or used by the **TARGET DEVICE**.

10. Evidence the **TARGET DEVICE** was attached to any other storage devices or similar containers for electronic evidence, to include other devices that connected via Bluetooth, direct connection, Airdrop, or another Wi-Fi/ Bluetooth enabled sharing app or capability between devices.

11. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage such as on a SIM card, SD card, and any photographic form.